A NEW SIGNING ALGORITHM BASED ON ELLIPTIC CURVE DISCRETE LOGARITHMS AND QUADRATIC RESIDUE PROBLEMS

Nedal Tahat

Department of Mathematics
Faculty of Sciences
The Hashemite University
Zarqa 13133
Jordan
e-mail: nedal@hu.edu.jo

Emad E. Abdallah

Department of Computer Information System
Faculty of Prince Al-Hussein Bin Abdallah II
for Information Technology
The Hashemite University
Zarqa 13115
Jordan
e-mail: emad@hu.edu.jo

Abstract. In this paper we propose a new digital signature algorithm for authenticity and integrity of a digital message. The core idea behind our approach is concentrated on using two hard problems in the signing process. The elliptic curve discrete logarithm and quadratic residue are engaged in a sophisticated manner to do the signing. The new proposed scheme provides higher level of security than other techniques that use a single hard problem. Clearly, Cybercriminals have to solve the two underlying hard problems simultaneously to destroy embedded signature. Extensive experimental results on several signed documents are performed to demonstrate the robustness of the proposed scheme against the most common attacks on digital signatures. Moreover, the computational complexity of the new scheme requires reasonable number of operations in both signing and verifying algorithms.**Keywords:** Cryptography, Digital Signature, Quadratic Residue, Elliptic Curve Discrete Logarithms, heuristically secure.

1. Introduction

In modern cryptography, the security and robustness of the digital signature algorithms are based on the difficulty of solving some hard theoretical problems such as factoring and discrete logarithm [2], [3], [14]. In the literature, various digital signature algorithms that use two theoretical hard problems [4], [5], [15] have been proposed. One common feature of these algorithms is that they are depending on a number-theoretical problem and thus their implementations depend heavily on modular exponentiation which is known to be time consuming with high computational complexity.

Elliptic curves are used in cryptography by Koblitz [7] and Miller [10] to overcome the costly modular exponentiation. The cryptographic schemes with security lie on the so-called elliptic curve discrete logarithm (ECDLP) [7], [10] are proved to provide longer security and better efficiency than both integer factorization system and discrete logarithm systems. The ECDLP has become a turning point of the rigorous development of cryptographic schemes [1], [9], [6], [13], [11], [12].

Motivated by the need for secure digital signature scheme,we propose a robust signature approach using the ECDLP and quadratic residue problem (QRP) hard problems. The new scheme offers better security than all other schemes based on either ECDLP or QRP. This is because the probability of solving two hard problems simultaneously by adversaries is believed to be negligible. Moreover, the proposed scheme does not involve any modular exponentiation operation in all algorithms. The remainder of this paper is organized as follows. In Section 2, we briefly review some background material and describe the ECDLP and QRP hard problems. In Section 3 we introduce the proposed approach and describe in detail the key generation, the signing and the verification algorithms. In Sections 4 and 5, we present some security analysis and the performance evaluation of the proposed approach. Finally, we conclude and point out future directions in Section 5.

1.1. Elliptic curve

In this section we describe some elementary tools on elliptic curves and define the two underlying hard problems ECDLP and QRP.

Definition 1.1 Let K be a field of characteristic neither of 2 nor 3, then an elliptic curve can be expressed as:

$$y^2 = x^3 + ax + b \tag{1.1}$$

where $a, b \in K$ and $4a^3 + 27b^2 \neq 0$. The set $E(K)$ consists of all point (x, y), $x, y \in K$ which satisfy the defining equation (1.1) together with a special point $\mathcal{O}$ called the point at infinity. Let G be a point on the elliptic curve defined in in equation (1.1) and if n is the smallest positive integer satisfying the equation $nG = \mathcal{O}$, then we say that G has an order n and is called the base point. See [6], [7], [8], [10] for complete discussion on how to add and to multiply elliptic curves points.

- ECDLP: Let G and C be two elliptic curve points on equation (1.1). Then find a positive integer k such that $kG = C$.

- QRP: Let p, q are two strong primes of large size and γ is an integer. Then compute an integer γ such that $\gamma \equiv \beta^2 \pmod{pq}$

2. The new signature scheme

The proposed signature scheme consists of four main phases: initialization, algorithm for key generation, algorithm for signing messages, and algorithm for signature verification.

2.1. Initialization

- The field $K = F_p$ of order p, where p is be a large prime number and $p-1$ have two prime factors $\bar{p}$ and $\bar{q}$.
- Two coefficient $a, b \in F_p$ that define the equation $y^2 = x^3 + ax + b (\bmod p)$ over F_p.
- $n = \bar{p}\bar{q}$, so that $n/(p-1)$ is a root points of elliptic curve construct a circulating subgroup. G is a generating element for subgroup and its rank equals n.
- $h(.)$ is a secure hash function.

2.2. Algorithm for generating keys

Step 1 Pick randomly two integers α and β from $\mathbb{Z}_n$

Step 2 Compute an integer k such that $k\alpha^{4\beta} \equiv -1 (\bmod n)$

Step 3 Calculate $T = kG$

The signer publishes his public keys as (p, G, n, T) and his corresponding private keys as (α, β, k).

2.3. Algorithm for signing message

Suppose the verifier wants the signer's signature on his message m. The signer then:

Step 1 Select an integer $r \in \mathbb{Z}_n$ such that $\gcd(r, n) = 1$

Step 2 Compute $R = r\beta^2 G = (x_1, x_2)$, where $u \equiv x_1 (\bmod n)$

Step 3 Calculate $s \equiv \frac{1}{2}(r + h(m)u^2\beta^2)(\bmod n)$

Step 4 Calculate $v \equiv \frac{1}{2}\alpha^{2\beta}(r - h(m)u^2\beta^2)(\bmod n)$

The original signer then produces (R, s, v) as a signature of message M.

2.4. Algorithm for verifying signature

Verifier tests the validity of the signature (R, s, v) by checking the following steps

Step 1 Compute $W_1 = s^2G + V^2T \pmod n$

Step 2 Compute $W_2 = h(m)u^2R \pmod n$

Accept the signature as valid if and only if $W_1 = W_2$

Theorem 2.1 *If the algorithms for keys and signing message are run smoothly then the validation of signature is correct.*

Proof. Squaring s and v

$$\begin{aligned} s^2 &\equiv \frac{1}{4}(r^2 + h(m)^2u^4\beta^4 + 2rh(m)u^2\beta^2) \pmod n \\ v^2 &\equiv \frac{1}{4}\alpha^{4\beta}(r^2 + h(m)^2u^4\beta^4 - 2rh(m)u^2\beta^2) \pmod n \end{aligned}$$

we have

$$s^2G = \frac{1}{4}(r^2 + h(m)^2u^4\beta^4 + 2rh(m)u^2\beta^2)G \pmod n$$

$$\begin{aligned} v^2T &= \frac{1}{4}\alpha^{4\beta}(r^2 + h(m)^2u^4\beta^4 - 2rh(m)u^2\beta^2)kG \pmod n \\ &= \frac{1}{4}k\alpha^{4\beta}(r^2 + h(m)^2u^4\beta^4 - 2rh(m)u^2\beta^2)G \pmod n \\ &= -\frac{1}{4}(r^2 + h(m)^2u^4\beta^4 - 2rh(m)u^2\beta^2)G \pmod n \end{aligned}$$

Thus

$$\begin{aligned} W_1 &= s^2G + v^2T \\ &= \frac{1}{4}(r^2 + h(m)^2u^4\beta^4 + 2rh(m)u^2\beta^2)G - \frac{1}{4}(r^2 + h(m)^2u^4\beta^4 - 2rh(m)u^2\beta^2)G \\ &= h(m)u^2r\beta^2G \\ &= h(m)u^2R \\ &= W_2 \end{aligned}$$

We accept the signature if $W_1 = W_2$. With the knowledge of the signer's public key (n, T) and the signature (R, s, v) of m, the verifier can authenticate the message m because the verifier can be convinced that the message was really signed by the signer. Else, the signature (R, s, v) is invalid.

3. Security analysis

One of the known models of security in cryptography is heuristic or ad-hoc model. We show that our scheme is heuristically secure by considering several possible attacks by an adversary (Adv). For every attack, we give valid reasons of why this attack fails.

Attack 1: Adv wishes to obtain secret keys (α, β, k) using all information available in the system. In this case, Adv needs to solve $T = kG \,(\bmod\, n)$ and $k\alpha^{4\beta} \equiv -1(\bmod\, n)$ which are clearly infeasible due to the difficulty of solving the ECDLP and factoring problem .

Attack 2: Adv tries to derive the signature (R, s, v) for a given message m by fixing the value of two integers in order to find the remaining one. In this case, Adv randomly fixes either (R, s) or (R, v) or (s, v) to find s, v or R respectively to satisfy $W_1 = W_2$. Obviously, this is as difficult as solving QRP and ECDLP simultaneously. For example, say Adv fixes the value (R, s) and tries to figure out the value of v . Adv then needs to solve the following equations that can be reduced from

$$s^2G + v^2T = h(m)u^2R \tag{2.1}$$

Adv start by computing

$$\gamma = v^2T$$

where γ is known and can be calculated easily. Note that, solving the above equation is as hard as solving ECDLP. But, even if ECDLP is solvable then the above equation is reducible to the next equation as below:

$$\lambda \equiv kv^2(\bmod\, n) \tag{2.2}$$

where λ is known but solving this equation is hard as solving the QRP.

Attack 3: Adv may also try collecting t valid signatures (R_j, s_j, v_j) on message M_j where $j = 1, 2, ..., t$ and attempts to find secret keys of the signature scheme. In this case, Adv has s equations as follows:

$$\begin{array}{rcl} s_1^2 + v_1^2k & = & r_1h(M_1)u_1^2\beta^2 \\ s_2^2 + v_2^2k & = & r_2h(M_2)u_2^2\beta^2 \\ & \vdots & \\ s_t^2 + v_t^2k & = & r_th(M_t)u_t^2\beta^2 \end{array}$$

In the above s equations, there are $(t + 2)$ variables that is k, β and r_j, where $j = 1, 2, ..., t$ which are unknown by the Adv. Hence, k and β remain hard to detect because Adv can generate infinite solutions of the above system of equations but cannot figure out which one is correct.

Attack 4: It is assumed that Adv is able to solve ECDLP problem. In this case, Adv knows k and $r\beta^2 \equiv \xi \,(\bmod\, n)$ but cannot figure out the values of r and β because breaking of QRP is difficult. Now from $s^2G + v^2T = h(m)u^2R$, Adv will have

$$s^2 + v^2k \equiv rh(m)u^2\beta^2(\bmod\, n) \tag{2.3}$$

Adv can launch Attack 2 but will not be successful due to the hardness of breaking QRP. Since Adv knows k, Adv may try to obtain α and β from equation

$$k\alpha^{4\beta} \equiv -1(\text{mod } n) \tag{2.4}$$

but still fail although Adv does know the factorization of n.

Attack 5: It is assumed that Adv is able to solve FAC problem. That means, he knows the prime factorization $\bar{p}$ and $\bar{q}$. In this case, Adv will learns nothing about k, α and β from the equation (2.4). Adv also has no information about k and (r, β) from equation (2.3) because there are three unknowns in the equation.

4. Performance evaluation

In this section we investigate the efficiency and the performance of our proposed scheme in terms of number of keys, computational complexity and communication costs. The complete lists of the notations that we used to analyze the performance are shown in Table 1.

Table 1: Lists of the notations that we used to analyze the performance of the proposed scheme

Notation	Description
SK	Number of secret keys
PK	Number of public keys
T_{mul}	The time complexity for executing the modular multiplication
T_{add}	The time complexity for executing the modular addition
T_{exp}	The time complexity for executing the modular exponentiation
T_{ec-add}	The time complexity for executing the addition of two elliptic curve points
T_{ec-mul}	The time complexity for executing the multiplication on elliptic curve points
T_{sqr}	The time for modular square computation
T_r	The time complexity for selecting a random integer
T_h	The time complexity for performing a one-way hash function h

The performance of our new signature scheme is summarized as follows: The number of keys in this scheme is given by $PK = 4$, and $SK = 3$. The signer needs $T_{ec-mul}+6T_{mul}+6T_{sqr}+T_{exp}+T_r+T_h$ time complexity to create a signature on any message, m.The signature validation verifier needs $3T_{ec-mul} + 3T_{sqr} + T_{mul} + T_h$. Finally the communication costs and the parameters for signing message and verifying signature are respectively given by $3|n|$ and $2|n|$.

To describe the efficiency performance in terms of T_{mul}, we use the conversion proposed in [8]. It converts various operations units to the time complexity for executing the modular multiplication.

$$T_{exp} \approx 240T_{mul};\ T_{ec-mul} \approx 29T_{mul};\ T_{ec-add} \approx 0.12T_{mul}$$

Assuming the time complexity for T_h and T_r are negligible, we found that, our signing message requires $275T_{mul} + 6T_{sqr}$ time complexity and our verifying signature requires $88T_{mul} + 3T_{sqr}$ time complexity. The widely used RSA signature scheme needs $240T_{mul}$ in both signature message and in its verifying signature. clearly our new proposed scheme is more efficient than RSA and yet our scheme is based on two hard problems which offer a longer security than RSA.

5. Conclusion

In this paper, we presented a new computationally inexpensive digital signature scheme based on the ECDLP and QRP problems. The new scheme offers higher level of security than other algorithms that based on ECDLP or QRP. The performance of the proposed method was evaluated through extensive experiments that clearly showed a perfect resiliency against a wide range of attacks including the key-only attack, ECDLP and QRP attacks, the chosen-message and feed attacks. Furthermore, it requires only minimal and acceptable number of operations in both signing and verifying algorithm.

References

[1] Chung, Y.F., Huang, K.H., Lai, F., Chen, T.S., *ID-based digital signature scheme on elliptic curve cryptosystem*, Computer Standards and Interfaces, 29 (6) (2007), 601-604.

[2] Diffie, W., Hellman, M., *New directions in cryptography,* IEEE Trans. Info. Theory, IT (31) (1976), 441-445.

[3] ElGamal, T., *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Info. Theory, IT (31) (1985), 479-472.

[4] Ismail, S.E., Yahya, A.H., *A new version of ElGamal signature scheme,* Sains Malaysian, 35 (2) (2006), 69-72.

[5] Ismail, S.E., Yahya, A.H., *Two new signature schemes based on the interactability of factoring a large composite number.* In the Proceeding of the First International Conference on Quantitative Sciences and Its Applications, UUM, Kedah, 2005, 1-8.

[6] Johnson, D., Menezes, A., Vanston, S., *The Elliptic Curve Digital Signature Algorithm,* International Journal of Information Security, 1 (1) (2001), 36-63.

[7] Koblitz, N., *Elliptic curve cryptosystems,* Mathematics of Computation, 48 (177) (1987), 203-209.

[8] Koblitz, N., Menezes, A., Vanstone, S., *The state of elliptic curve cryptography,* Design, Code Cryptography, 19 (2000), 173 -193.

[9] Liu, D., Huang, D., Dai, Y., Luo, P., *New Schemes for Sharing Points on an Elliptic Curve,* Computers and Mathematics with Application, 56 (2008), 1556-1561.

[10] Miller, V., *Uses of elliptic curves in cryptography,* Advances in cryptology-Crypto '85, LNCS, 218 (1986), 417426.

[11] Nikooghadam, M., Bonyadi, R.M., Malekian, E., A. Zakerolhosseini, A., *A protocol for digital signature based on the elliptic curve discrete logarithm problem,* Journal of Applied Sciences, 8 (10) (2008), 1919-1925.

[12] Popescu, C., *An identification scheme based on the elliptic curve discrete logarithm problem,* In the Proceedings of The 4th International Conference on High-Performing Computing in the Asia-Region, 2 (2000), 624-625.

[13] Rabah, K., *Elliptic curve ElGamal encryption and signature schemes,* Information Technology Journal, 13 (3) (2005), 299-309.

[14] Rivest, R., Shamir, A., Adleman, L., *A method for obtaining digital signature and public key cryptosystem,* Communication of the ACM, 21 (1978), 120-126.

[15] Tahat, N., Ismail, S.E., Ahmad, R.R., *A new signature scheme based on factoring and discrete logarithms,* Journal of Mathematics and Statistics, 4 (4) (2008), 222-225.

Accepted: 09.03.2013